UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/821,754	03/30/2001	Matthew N. Schmid	CIG-101	5170

28970 7590 03/07/2005

SHAW PITTMAN
IP GROUP
1650 TYSONS BOULEVARD
SUITE 1300
MCLEAN, VA 22102

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/821,754	SCHMID ET AL.	
	Examiner	Art Unit	
	Ellen C Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 October 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: 27 October 2004, with an original filing date of 31 March 2000.

2. Claim 1 has been canceled. Claims 2-21 have been added.

3. Claim 2-21 are currently pending in this application. Claims 2, 12, and 20 are independent claims.

Response to Arguments

4. Applicant's arguments with respect to claims 2-21 have been considered but are moot in view of the new ground(s) of rejection, which was necessitated by amendment.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 2-21** are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. U.S. Patent No. 6,298,445 (hereinafter '445) in further view of Gooderum et al. U.S. Patent No. 6,219,707 (hereinafter '707).

As to independent claim 2, "A method for preventing process creation of an unauthorized user application executable by an operating system of a computer, comprising:" is taught in '445 col. 2, line 60 through col. 3, line 6 "In another aspect, the

invention relates to a network security detector that is used to monitor security intrusions on a network ...and a fifth application responsible for receiving the software enhancements";

"intercepting a request for execution of an application executable by a user using the substitute process creation function" and **"comparing the information to a list of authorized executables for the user using the usermode application"** is shown in '445 col. 8, lines 9-54 "The push system integrates the software enhancement in to existing programs. Additionally, the integration can also perform a check on the integrity and authenticity of the software enhancement provided. This feature determines whether the user being sent the software enhancement is eligible, and chick the integrity and authenticity of the software enhancement"

"communicating information about the request from the substitute process creation function to a user-mode application running as a service" is disclosed in '445 col. 7, lines 55-65 "The push system automatically implements and electronically sends computer software enhancements over a computer network when the software enhancement becomes available. The software enhancement can include an update to a computer security vulnerabilities database or a new version of an entire computer security software package";

"if the information does not match an item on the list, communicating a first message to deny the request from the user-mode application to the substitute process creation function; and if the information does match an item on the list, communicating a second message to permit the request from the user-mode application to the substitute process creation function" is taught in '445 col. 8, lines 3-6 "If the enhancement is available,

the server either pushes the enhancement over the network to the user or provides a negative response is it cannot push the enhancement for some reason";

the following is not taught in '445: **"inserting into a kernel of the operating system a substitute process creation function"** however '707 teaches "In that embodiment, BSD386 is hardened by adding a type enforcement mechanism which restricts the access of processes to data ... To accomplish this, system calls in the basic BSD386 kernel were modified so that type enforcement checks cannot be avoided. Certain other system calls were either disabled or had certain options disabled" in col. 3, lines 26-37.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '445 that teach a method for computer network security to include a means to protect the kernel of the operating system. One of ordinary skill in the art would have been motivated to perform such a modification to protect a computer network from attack by malicious outsiders (see '707 col. 1, lines 23 et seq.). "To protect themselves from attacks by malicious outsiders, organizations are turning to mechanisms for increasing network security. One such mechanism is described in "SYSTEM AND METHOD FOR PROVIDING SECURE INTERNETWORK SERVICES", U.S. patent application Ser. No. 08/322,078 filed Oct. 12, 1994 by Boebert et al., the discussion of which is hereby incorporated by reference. Boebert teaches that modifications can be made to the kernel of the operating system in order to add type enforcement protections to the operating system kernel. This protection mechanism can be added to any other program by modifications to the program code made prior to compiling. It cannot, however, be used to add type enforcement protection to program code after that program code has been compiled".

As to dependent claim 3, "wherein the inserting into a kernel of the operating system a substitute process creation function comprises: creating a device driver; loading the device driver into the kernel; and modifying a table consulted by a dispatcher using the device driver" is taught in '445 col. 8, lines 19-40 "The push system integrates the software enhancement into existing programs".

"wherein the modifying a table causes the dispatcher to call the substitute process creation function in place of a second process creation function" is shown in '445 col. 10, line 21 through col. 11, line 61 "After storing the software enhancemnt with the client , the installer 58 updates an archive (Step 118), overwrites any previously existing software enhancement packages (Step 120)".

As to dependent claim 4, "wherein the loading the device driver comprises one of dynamically loading into the kernel and loading into the kernel as part of a boot sequence" is disclosed in '707 col. 4, lines 6-22 "On the other hand, the operational kernel is subject to type enforcement. This means, for instance, that executable files stored in the memory of the secure computer cannot be executed without explicit execution privileges. In one such embodiment, executable files cannot be give execution privileges from within the operational kernel. Instead, the secure computer must enter administrative kernel to grant execution privileges. This prevents execution of malicious software posted to memory of the secure computer. Instead, only executables approved by operational administrators while in administrative kernel mode ever become executable within operational kernel mode of the secure computer. In one such embodiment, administrative kernel can be entered only from

either a manual interrupt of the boot process to boot the administrative kernel or by booting the secure computer from a floppy that has a pointer to the administrative kernel".

As to dependent claim 5, "wherein the substitute process creation function is a wrapper around a process creation function provided by the operating system" is taught in '707 col. 3, lines 19-25 "In one embodiment, a tcp wrapper package operating in the Internet protocols is used to sit on the external, public network so that information about external probes can be logged. It is most likely that the open nature of the public network will favor the use of public-key cryptography in this module".

As to dependent claim 6, "wherein the process creation function provided by the operating system comprises ZwCreateProcess" is shown in '445 col. 8, lines 41-54 "The Push Mechanism ... delivers the software enhancement to the customer and invokes and installer 58 via the update processor 54".

As to dependent claim 7, "wherein the information comprises one or more of a user name, an application executable name, and a cryptographic identifier of an application executable" is disclosed in '445 col. 8, lines 19-31 "Additionally, the integration can also perform a check on the integrity and authenticity of the software enhancement provided. This feature determines whether the user being sent the software enhancement is eligible, and checks the integrity and authenticity of the software enhancement. In determining the integrity and authenticity of the software enhancement, the push system can use digital signatures or other cryptographic techniques".

As to dependent claim 8, "wherein the cryptographic identifier of an application executable comprises a hash created using; an MD5 cryptographic algorithm" is taught in

'445 col. 11, lines 17-31 "The message that is signed is typically a condensed version of the actual message produced by a message digest (MD) or hash algorithm. In general, a message digest algorithm, takes as an input a message of arbitrary length and produces a shorter fingerprint of the input. In the disclosed invention, the message digest algorithm used is called MD5 and produces a 128-bit fingerprint".

As to dependent claim 9, "wherein the list comprises one or more of an application executable name and a cryptographic identifier of an application executable" is shown in '445 col. 10, lines 21-60 "Prior to installing the software enhancement on a computer or on a local server 18, the authenticity and integrity of the software enhancement is determined. The authenticity checks may occur either at user's computer or at the local server 18. The authenticity checks include performing a cryptographic technique by verifying the user before installing the software enhancement"

As to dependent claim 10, "wherein the comparing the information to a list comprises comparing an application executable name of the information with an application executable name of at least one item from the list" is disclosed in '445 col. 10, lines 21-60.

As to dependent claim 11, "wherein the comparing the information to a list comprises comparing a cryptographic identifier of the information with a cryptographic identifier of at least one item from the list" is taught in '445 col. 10, lines 21-60.

As to dependent claim 12, "wherein the communicating information about the request comprises one or more of releasing a semaphore, calling an application program interface function, polling, using a socket, and using a pipe" is shown in '707 col. 3,

lines 37-52 "The type enformcement controls are enforced by the kernel and connot be circumvented by applications. Type enforcement is used to implement data flow structures call Assured Pipelines".

As to dependent claim 13, "wherein the communicating a first message to deny the request comprises one or more of calling an application program interface function, polling, using a socket, and using a pipe" is disclosed in '707 col. 3, lines 37-52.

As to dependent claim 14, "wherein the communicating a second message to permit the request comprises one or more of calling an application program interface function, polling, using a socket, and using a pipe" is taught in '707 col. 3, lines 37-52.

As to independent claim 15, "A method for preventing process creation of an unauthorized user application executable by an operating system of a computer, comprising" is taught in '445 col. 2, line 60 through col. 3, line 6;

"inserting into a kernel of the operating system a substitute process creation function" is shown in '707 col. 3, lines 26-37;

"intercepting a request for execution of an application executable by a user using the substitute process creation function; communicating information about the request from the substitute process creation function to a user-mode application running as a service; prompting the user for authorization to proceed using the user-mode application" is shown in '445 col. 8, lines 9-54;

"if the authorization is not provided, communicating a. first message to deny the request from the user-mode application to the substitute process creation function; and if the authorization is provided, communicating a second message to permit the request from

the user-mode application to the substitute process creation function" is taught in '445 col. 8, lines 3-6

As to dependent claim 16, "wherein the authorization comprises a password" is shown in '707 col. 25, lines 10-15 "The rest of the installation is HTML forms-driven through the browser. Various items such as port number for the Commerce server, UID to run the server under, install directory, logging, administration password, and other server configuration are entered via three forms".

As to dependent claims 17-19, these claims are substantially similar to claims 3-5; therefore they are rejected along similar rationale.

As to independent claim 20, this claim is directed to a system of the method of claim 2; therefore it is rejected along similar rationale.

As to dependent claim 21, "further comprising an administrative server, wherein the administrative server is in communication with the user-mode application, and wherein the usermode application downloads the list from the administrative server" is taught in '445 col. 2, lines 47-53 "In one aspect, the invention provides the most recent information regarding new security attacks. A user can either request the enhancement, or it can be automatically sent (e.g., via the internet) when it becomes available".

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen. Tran
Patent Examiner
Technology Center 2134
28 February 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100